



**Information Operations Vulnerability/Survivability
Assessment (IOVSA):
Process Structure (Revision A)**

**Arturo Revilla, Nora Christianson, Eric Gunderson,
Cruz Ochoa, Rick zum Brunnen, and Thomas McDonald**

ARL-TR-2993

June 2003

NOTICES

Disclaimers

The findings in this report are not to be construed as an official Department of the Army position, unless so designated by other authorized documents.

Citation of manufacturers' or trade names does not constitute an official endorsement or approval of the use thereof.

The findings in this report are not to be construed as an official Department of the Army position, unless so designated by other authorized documents.

Army Research Laboratory

White Sands Missile Range, NM 88002-5513

ARL-TR-2993**June 2003**

Information Operations Vulnerability/Survivability Assessment (IOVSA): Process Structure (Revision A)

**Arturo Revilla, Nora Christianson, Eric Gunderson,
Cruz Ochoa, Rick zum Brunnen, and Thomas McDonald**
Survivability/Lethality Analysis Directorate
Information & Electronic Protection Division

| REPORT DOCUMENTATION PAGE | | | | Form Approved OMB No. 0704-0188 | |
|--|------------------|-------------------------|---|--|--|
| Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing the burden, to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS. | | | | | |
| 1. REPORT DATE (DD-MM-YYYY) June 2003 | | 2. REPORT TYPE Final | | 3. DATES COVERED (From - To) May 2002 – February 2003 | |
| 4. TITLE AND SUBTITLE Information Operation Vulnerability/Survivability (IOVSA): Process Structure (Revision A) | | | | 5a. CONTRACT NUMBER | |
| | | | | 5b. GRANT NUMBER | |
| | | | | 5c. PROGRAM ELEMENT NUMBER | |
| 6. AUTHOR(S) Arturo Revilla, Nora Christianson, Cruz Ochoa, Eric Gunderson, Rick zum Brunnen, and Thomas McDonald | | | | 5d. PROJECT NUMBER | |
| | | | | 5e. TASK NUMBER | |
| | | | | 5f. WORK UNIT NUMBER | |
| 7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) U.S. Army Research Laboratory Information & Electronic Protection Division Survivability/Lethality Analysis Directorate (ATTN: AMSRL-SL-EA) White Sands Missile Range, NM 88002-5513 | | | | 8. PERFORMING ORGANIZATION REPORT NUMBER ARL-TR-2993 | |
| 9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) U.S. Army Research Laboratory 2800 Powder Mill Road Adelphi, MD 20783-1145 | | | | 10. SPONSOR/MONITOR'S ACRONYM(S) ARL/SLAD/IEPD, APG, MD | |
| | | | | 11. SPONSOR/MONITOR'S REPORT NUMBER(S) ARL-TR-2993 | |
| 12. DISTRIBUTION/AVAILABILITY STATEMENT Approved for public release; distribution unlimited. | | | | | |
| 13. SUPPLEMENTARY NOTES | | | | | |
| 14. ABSTRACT This report details the revised IOVSA process and supersedes the previous methodology, "IOVSA: Process Structure", ARL-TR-2250, dated June, 2000. The objective of the methodology remains the same as its predecessor, i.e., to provide a solid foundation for the evaluation of DoD Information Technology (IT) based systems and the commercial IT-based systems that support them. | | | | | |
| 15. SUBJECT TERMS Vulnerability, survivability, susceptibility, Information Operations | | | | | |
| 16. SECURITY CLASSIFICATION OF: | | | 17. LIMITATION OF ABSTRACT SAR | 18. NUMBER OF PAGES 29 | 19a. NAME OF RESPONSIBLE PERSON Thomas McDonald |
| a. REPORT U | b. ABSTRACT U | c. THIS PAGE U | | | 19b. TELEPHONE NUMBER (Include area code) (505)678-2324/DSN258-2324 |

Contents

| | |
|--|-----------|
| Report Documentation Page | ii |
| Summary | 1 |
| 1. Introduction | 2 |
| 1.1 Scope | 3 |
| 1.2 SLAD Background | 3 |
| 2. IOVSA Methodology | 4 |
| 2.1 Phase I: System Familiarization | 6 |
| 2.1.1 Introduction | 6 |
| 2.1.2 Rationale..... | 7 |
| 2.1.3 Objectives | 7 |
| 2.1.4 Deliverables..... | 7 |
| 2.2 Phase II: System Design/Functionality Analysis | 8 |
| 2.2.1 Introduction | 8 |
| 2.2.2 Rationale..... | 8 |
| 2.2.3 Objectives | 9 |
| 2.2.4 Deliverables..... | 9 |
| 2.3 Phase III: Threat Analysis | 9 |
| 2.3.1 Introduction | 9 |
| 2.3.2 Rationale..... | 10 |
| 2.3.3 Objectives | 10 |
| 2.3.4 Deliverables..... | 10 |
| 2.4 Phase IV: Susceptibility Analysis | 11 |
| 2.4.1 Introduction | 11 |
| 2.4.2 Rationale..... | 13 |
| 2.4.3 Objectives | 13 |
| 2.4.4 Deliverables..... | 13 |
| 2.5 Phase V: Vulnerability Risk Assessment | 14 |
| 2.5.1 Introduction | 14 |

| | | |
|-----------|-------------------|-----------|
| 2.5.2 | Rationale..... | 14 |
| 2.5.3 | Objectives..... | 14 |
| 2.5.4 | Deliverables..... | 15 |
| 3. | DITSCAP | 15 |
| 4. | Conclusion | 18 |
| 5. | References | 19 |
| | Acronyms | 20 |

List of Figures

| | | |
|-----------|-------------------------------------|---|
| Figure 1. | Interrelation of IOVSA phases | 4 |
| Figure 2. | IOVSA phase breakout structure..... | 5 |

List of Tables

| | | |
|----------|--|----|
| Table 1. | IOVSA phases..... | 4 |
| Table 2. | Relationship of the IOVSA methodology process to DITSCAP phases, activities and tasks..... | 16 |

Summary

This document is a revision of the IOVSA methodology formalized in June 2000. The goal of this revised document will be the clarification of the work to be performed for each phase, the requirements, and the expected deliverables. Since this revision will be a living document, it will be updated as appropriate to include lessons learned. The intent of this revision is to facilitate the dialog between the U.S. Army Research Laboratory/Survivability Lethality Analysis Directorate (ARL/SLAD) and the decision-makers (Program Executive Offices (PEOs), Program Managers (PMs), evaluators, contractors, etc.) for U.S. Army IT-based systems.

As before, the IOVSA process will provide a structured methodology for assessing IT system/System of Systems (SoS) IO susceptibilities and vulnerabilities. The process will provide flexibility that enables the analyst to customize it for the system/SoS under assessment. Additionally, the IOVSA results will provide critical information to system developers and decision-makers regarding the system's/SoS' IO susceptibilities and vulnerabilities. Furthermore, enough information will be able to be extracted from the process to evaluate different countermeasure techniques and protection recommendations to determine their feasibility and cost/reward ratio.

In summary, the IOVSA process will provide the framework for a consistent and rigorous vulnerability assessment of a system/SoS in order to determine its IO areas of concern, and to discern the appropriate actions to protect and enhance soldier and system survivability.

1. Introduction

In June of 2000, the Army Research Laboratory (ARL) Survivability/Lethality Analysis Directorate (SLAD) formalized a methodology for the evaluation of U.S. Department of Defense (DoD) information technology (IT)-based systems, which encompass both non-weapon elements (All Source Analysis System (ASAS), Combat Service Support Control System (CSSCS), Force XXI Battle Command Battalion/Brigade and Below (FBCB2), etc.), as well as weapon platforms such as Stryker or Comanche. The methodology, known as the Information Operations Vulnerability/Survivability Assessment (IOVSA), provides a structured process for the evaluation of DoD IT systems at any point during their acquisition life cycle. In addition, the IOVSA process complements the DoD IT Security Certification and Accreditation Process (DITSCAP) by fulfilling many of the DITSCAP requirements (*1*).

With regard to information operations (IO), SLAD's goal is to enhance the overall survivability of IT-based systems and System of Systems (SoS). Henceforth, any reference to 'IT based Systems' in the remainder of the document will encompass both individual systems and SoS. To this end, the IOVSA process investigates the DoD and U.S. Army information assurance (IA) criteria that are mandatory for IO vulnerability and survivability assessments of IT-based systems and SoS. These criteria include:

- Availability
- Confidentiality
- Identification
- Integrity
- Non-repudiation

Over the course of ten years, SLAD analysts have effectively applied the IOVSA methodology to various systems/SoS. With this experience, SLAD undertook a review of the IOVSA process to (1) ensure that it would continue to be relevant as IT-based systems and networks become more sophisticated, and (2) to identify minor adjustments to the process that would enhance the IOVSA product.

The in-depth review resulted in a revision to the original IOVSA process. This report contains the revised IOVSA methodology, relevant explanations of the methodology phases, and references to documentation that aids in conducting the IOVSA phases.

The revision, contained herein, (1) clarifies the process and (2) will assist the Program Executive Officer (PEO), Project Manager (PM), or contractor representative to understand the benefits of the IOVSA methodology, the requirements for the proper evaluation of the system/SoS, and the

expected deliverables to his/her office. ARL/SLAD is confident that, with the proper understanding of the methodology and its requirements, the products generated will continue to improve.

1.1 Scope

This report details the revised IOVSA process and supersedes the previous methodology documented in *Information Operations Vulnerability/Survivability Assessment (IOVSA): Process Structure* (2). While the revision process was extensive, the resultant methodology remains very similar to the previous work. Those familiar with the original methodology will find many similarities between the previous version and this one. It is the authors' hope that the revised process addresses some of the shortcomings of the original methodology, and provides clarification of the methodology phases, their requirements, and their deliverables. The objective of the methodology remains the same as before, that is, to provide a solid foundation for the evaluation of DoD IT-based systems and the commercial IT-based systems that support them.

1.2 SLAD Background

SLAD is the U.S. Army's primary source for survivability, lethality, and vulnerability (SLV) analysis and evaluation support. To this end, SLAD's objective, to ensure that soldiers and systems can survive and function on the battlefield, is accomplished by:

1. Providing SLV analysis and evaluation support over the entire life cycle of major U.S. Army systems, and helping to acquire systems that will survive and/or be highly lethal in all environments against the full spectrum of battlefield threats.
2. Providing advice/consultation on SLV issues to Headquarters Department of the Army (HQDA), PEOs/PMs, evaluators, combat developers, battle labs, intelligence activities, other U.S. Department of the Army (DA) and DoD activities, contractors, and Lead System Integrators (LSIs).
3. Conducting investigations, experiments, simulations, and analyses to quantify SLV of U.S. Army and selected foreign weapon systems.
4. Providing well-documented, timely technical judgments on complex SLV issues.
5. Performing special studies and making recommendations regarding tactics, techniques, or design modifications to reduce vulnerability and enhance survivability and lethality of U.S. Army materiel.
6. Developing tools, models, and methodologies (TMM) for improving SLV analysis.

SLAD has leveraged its traditional technical strengths in electronic warfare, networking, directed energy, high speed computation, military communications, the employment of U.S. Army systems, and systems engineering and analysis in order to develop one of the nation's premier capabilities in IO.

2. IOVSA Methodology

The IOVSA methodology (or process) is divided into five major phases. The phases are outlined in table 1, and their interrelation is illustrated in figure 1.

Table 1. IOVSA phases.

| Phase | Phase Title |
|-------|--------------------------------------|
| I | System Familiarization |
| II | System Design/Functionality Analysis |
| III | Threat Analysis |
| IV | Susceptibility Analysis |
| V | Vulnerability Risk Assessment |

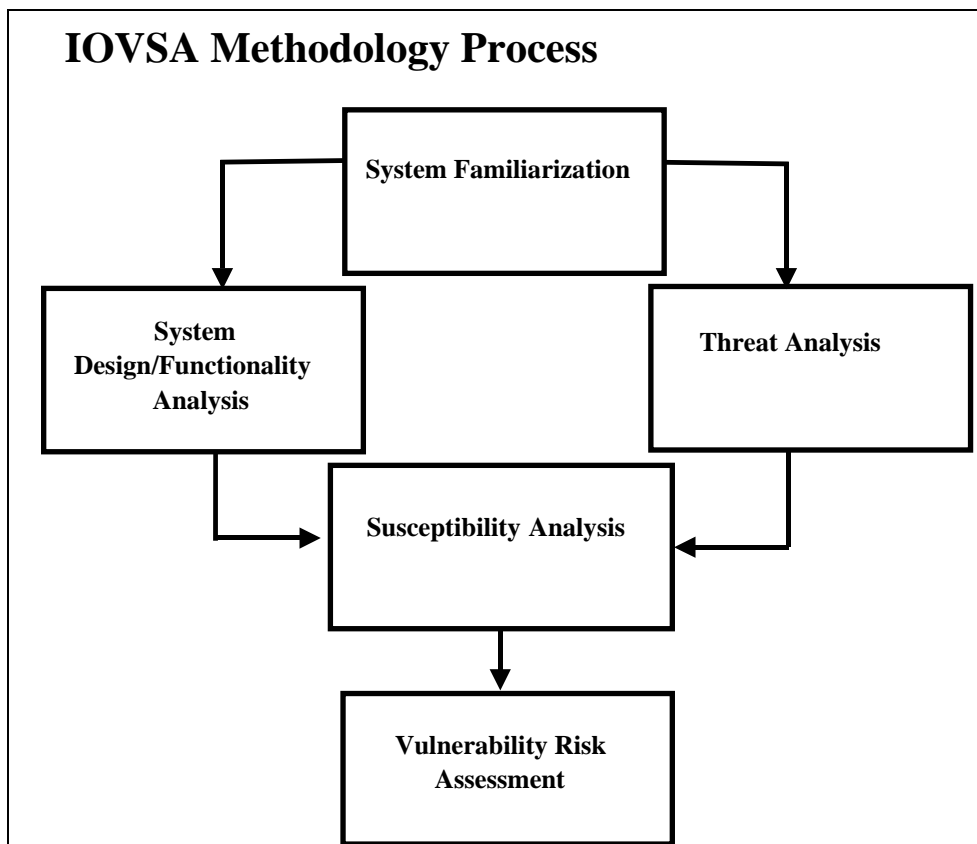


Figure 1. Interrelation of IOVSA phases.

Each of the phases is subdivided into appropriate sub-blocks. The sub-blocks identify the work that must be completed in the phase. Figure 2 illustrates the sub-blocks for each phase.

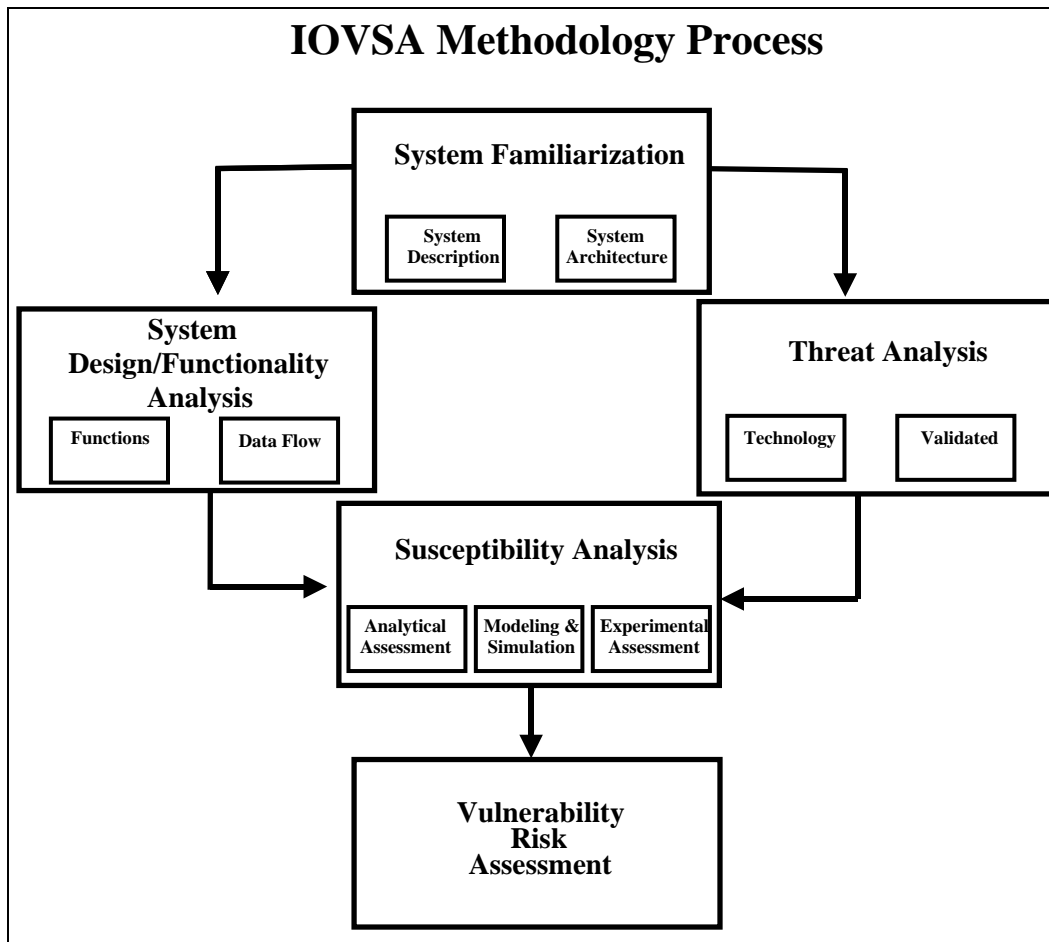


Figure 2. IOVSA phase breakout structure.

While the IOVSA process consists of five phases, the applicability of each phase to a DoD IT-based system is dependent upon the system issues, such as the system maturity, whether the system is assessed as an independent component or as part of a SoS analysis. The joint decision will be influenced by the mission requirements and the level of analysis required by the PEO/PM. In addition, customer requirements assist in focusing which phase is applicable to a specific assessment.

The IOVSA process is a living process in which the output of one phase may influence the amount of coverage and depth of another. The revised process allows this interaction to occur, and enables the analyst to customize the IOVSA as necessary. For example, the analyst and the PEO/PM may agree to limit the system familiarization (phase I) and system design/functionality analysis (phase II) to the minimum level of detail required to determine the system's (hardware and software) mission-critical resources. Similarly, the modeling and simulation process (phase IV) may be impractical for all IT-based systems given the current capabilities of existing force-on-force models to incorporate IO considerations (3). SLAD has developed a set of internal processes for conducting each of the IOVSA phases to help the SLAD analyst determine which phases are appropriate for the system under investigation.

The subsequent sections within this chapter provide an overview of each IOVSA phase to include the general goals and rationale. Information collected during the first phase of the IOVSA (when applicable), and an understanding of the goals and objectives of the other phases, will enable the analyst to determine and plan work for the relevant subsequent phases. It is important to note that the flexibility provided by the IOVSA process makes it practical to perform an evaluation without complete coverage of all phases.

2.1 Phase I: System Familiarization

2.1.1 Introduction

The IOVSA process begins with the accumulation of available information related to the IT-based system. This information includes specific technical data, performance requirements, environment descriptions, program definition, planning information, IO strategies, and operational requirements. In addition to gathering and reviewing information, the analyst will communicate with the customer (i.e., PEO or the PM office and/or LSI), prime/sub contractors) as required.

In order to complete phase I, SLAD will require the cooperation and participation of outside agencies and individuals. These resources will be used to identify the following:

- a. System mission
- b. System requirements
- c. System specifications
- d. IA requirements
- e. Data access policies
- f. Physical characteristics

During the research portion of the system familiarization, the analyst will also identify sources of information to be used in subsequent IOVSA phases, and will customize the methodology as appropriate.

The system familiarization phase consists of two components or sub-blocks: system description and system architecture. The system description provides the analyst with an understanding as complete as possible of the system and/or SoS under review. This understanding is essential to the successful application of the IOVSA methodology.

The system architecture is typically a high-level overview of the types of hardware, software, firmware, and associated interfaces envisioned for the system. This architecture description should contain an overview of the internal system structure and external network architecture, to include:

- Anticipated hardware configuration
- Application software
- Software routines
- Operating systems
- Remote devices
- Communications processors and protocols
- Network
- Remote interfaces

2.1.2 Rationale

Phase I of the IOVSA process is critical to the successful application of the methodology to a particular system. In this phase, a detailed description of the system or SoS under analysis is developed. This description is extremely important; it is the foundation upon which the subsequent IOVSA efforts will be based. During this phase, the analyst will determine the extent to which IOVSA efforts on other systems may be leveraged. The review of the documentation is necessary in order to properly identify the anticipated environments in which the system is to operate, as well as the mission requirements of the system. These details, as well as others, serve as inputs to the vulnerability risk assessment (phase V). The products of this phase are considered “living documents” and will be updated as appropriate due to architecture changes.

2.1.3 Objectives

The primary objective of this phase of the IOVSA process is to familiarize the SLAD analyst with the system under investigation. This familiarization is focused on the system’s physical configuration and interconnections, IT components (hardware and software), networking, electronics, power, and external network interfaces, as applicable. The system familiarization characterizes the system that will be analyzed throughout the remainder of the IOVSA process.

2.1.4 Deliverables

The deliverables for IOVSA phase I include, but are not limited to:

- a. A system familiarization report that summarizes the analyst’s understanding of the system’s mission, requirements, intended operational environment, as well as the physical configuration and interconnections of the system’s IT components (hardware and software), networking, electronics, and power.

- b. A proposed plan/schedule for conducting the other IOVSA phases. This schedule will identify other IOVSA efforts and schedules that may be leveraged to support the analysis. The plan/schedule developed is preliminary, and, as such, it is subject to change.

2.2 Phase II: System Design/Functionality Analysis

2.2.1 Introduction

The system design/functionality analysis is comprised of two components: a system functionality assessment and a data flow analysis. This phase of the IOVSA process is concerned with determining the functions or aspects of the system that enable it to complete its mission, and describing the information (or data) flow within the system and with external interfaces. The purpose of the data flow effort is to gain a detailed understanding of how information flows into, out of, and within the system.

The system functionality assessment provides a high level view of the system under investigation, with respect to its ability to perform its mission. The requirements identified in the phase I resource material (i.e., Operational Requirements Documents, etc.) are reviewed to determine the hardware/software implementations which support the various mission functions. The system functionality assessment will be used in IOVSA phases IV and V in order to determine a system's response to threat events. This functionality assessment will also provide insight on a degraded system's performance.

During the data analysis, the analyst will develop data flow diagrams, data dictionaries and transform descriptions. The data flow diagrams will depict each interface flow and data stores on each diagram. The data dictionary will document the content of the interface flows and data stores. The transform descriptions will visually depict the data flow process in a rigorous fashion, showing data message paths and timing information.

2.2.2 Rationale

The need for a detailed data (information) flow analysis depends upon the system and its mission. Additionally, the level of detail will also be system/scenario-specific. Since threats can affect information links and/or subsystems, it's not only important to know *how* the threat "couples" with the system, but also *when* the threat event occurs. The IT and electronic architecture is based upon a time sequence of process states. The state in which a system ends up depends upon what state the system was in when perturbed by the threat. The data flow analysis is the point in the IOVSA process where the "timing" factor is introduced. A secondary purpose of the data flow analysis is to obtain input for use in future modeling and simulation (M&S) efforts. In this case the data flow analysis will serve as a detailed program specification for the M&S efforts developed in IOVSA phase IV.

2.2.3 Objectives

The objective of the system functionality assessment portion of this phase is to determine the system's ability to perform its mission under IO. A second objective is to understand and document the system's internal and external information (data) flow.

2.2.4 Deliverables

Phase II will be documented in a report. The report will contain the system functionality assessment and the data flow analysis. The system functionality assessment portion will identify the system requirements and specifications, correlated with critical mission functions. The data analysis portion will contain data flow diagrams, data dictionaries and transform descriptions.

2.3 Phase III: Threat Analysis

2.3.1 Introduction

The threat analysis plays the critical role of determining the characteristics, tools and methodologies that an attacker may use to adversely affect the mission performance and, hence, survivability of an IT-based system and/or SoS. The threat analysis plays an important part for both the susceptibility assessment (phase IV) and the vulnerability risk assessment (phase V) by narrowing the field of threats and enabling the analysts to focus on those with an anticipated impact upon the system.

Historically, DoD and the U.S. Army have defined specific threat classes based upon the impact to the IT-based system. These classes include:

- The compromise or exploitation of information
- The corruption of information with loss of data integrity
- The destruction or modification of information
- The denial or interruption of service
- The physical destruction of the system

Some of the threat mechanisms that may be considered when determining the threats include, but are not limited to:

- Unauthorized access
- Authorized access
- Malicious software
- Signal intelligence (SIGINT)

- Radiation intelligence (RINT)
- Electronic attack
- Conventional weapons
- Nuclear electromagnetic pulse (EMP)
- Directed energy weapons (DEW)
- Non-nuclear EMP
- Obscurants
- Biological/chemical
- Other (theft, human error, etc.)

Validated threat documents, which relate the threat classes and mechanisms to individual IT-based systems, are oftentimes unavailable or not validated. In general, the analyst will be required to make a determination regarding what is technologically feasible in the absence of hard intelligence data or validated threat information. SLAD will continue to work with the intelligence community, Computer Emergency Response Teams (CERT), and the research community to ensure that the most current and technologically feasible, as well as validated, threats to the IT-based systems are considered during the threat analysis.

2.3.2 Rationale

The identification of system threats is an important step in the IOVSA process. The threat analysis provides critical information that ensures the proper development of a vulnerability risk assessment (phase V), and the proper conduct of the susceptibility assessment (phase IV). It is the process that gives credibility to the IOVSA evaluation.

2.3.3 Objectives

The objective of this phase is to identify threats to the system under evaluation, and to determine the likelihood of encounter for the threats. The likelihood of encounter will be used during phase V, the vulnerability risk assessment. The likelihood of encounter will take into account factors such as the system's/SoS' operational environment, the manner in which a system is deployed, and training, tactics and procedures (TTPs).

2.3.4 Deliverables

The threat analysis will be documented either in a stand-alone document, or as part of the susceptibility and/or vulnerability risk assessment report(s).

2.4 Phase IV: Susceptibility Analysis

2.4.1 Introduction

System/SoS susceptibilities are identified in the susceptibility assessment phase. Susceptibility is defined as any characteristic of an information-based system that has the potential for exploitation by an enemy.

Individual system components as well as the overall system/SoS are examined in the process. Due to the technical nature of susceptibilities, a large number of sources are used in the generation of the susceptibility profile for the system. Some of the sources include:

- a. Open source publications
- b. Past tests results on systems
- c. Other organizations such as the National Security Agency, the Defense Intelligence Agency, and the Department of Energy
- d. Hacker databases
- e. System developers' databases
- f. The Federal Bureau of Investigation (National Protection Center) database
- g. System configuration parameters
- h. Network connectivity information
- i. CERT
- j. IO laboratories such as SLAD, ARL, and Defense Advanced Research Projects Agency (DARPA)
- k. IOVSA experiments

The susceptibility profile is then used in conjunction with the threat analysis (phase III) in determining the system's vulnerabilities. The susceptibility assessment is divided into three separate blocks: an analytical assessment, modeling and simulation, and an experimental assessment.

An analytical assessment consists of inferring susceptibilities of the system by examining the design of its components. A review of available documentation, coupled with the information gathered from phase I of the IOVSA, is utilized to conduct a preliminary assessment. This assessment can also be based on previous experimental results from similar systems. An analytical susceptibility assessment allows for the leveraging of accumulated knowledge regarding previously identified system susceptibilities for the purpose of assessing analogous susceptibilities in the system under consideration. The output from the analytical assessment

process forms the foundation for the experimental assessment process and is useful for the prediction and confirmation of results found from the modeling and simulation process.

The purpose of the modeling and simulation process is to build a simulation of the system to accurately predict, classify and/or verify the information flow of the system under assessment. The information flow modeling approach has the potential of being of great benefit to the platform/node developers and the analyst. One of these benefits is in the area of testing where planned modifications to system software can actually be analyzed before programming the intended change. The functionality of the planned change can be incorporated into an information flow model environment to determine whether additional susceptibilities are introduced from these changes. This approach will not only save the platform/node developers' programmer time, it will also reduce the time demands of resources such as a system integration laboratory (SIL), which is used to ensure that the actual platform or node functions correctly and reliably.

Modeling and simulation present several advantages for vulnerability and survivability assessment work. It is nondestructive, usually cost effective, and flexible enough to accommodate new real-world data. It is also ideal for predicting susceptibilities and vulnerabilities in the composite environment found on Defense Department systems, support systems, and their components involved in battlefield operations.

The experimental assessment portion of the IOVSA process consists of an actual field or laboratory IO experiment to determine susceptibilities. If an analytical assessment has been done, the results can be used as guidance for planning of IO experiments. If a model of the system/SoS exists, the experimental assessment can be used to confirm the predicted results from the analytical susceptibility assessment.

Experiments typically involve a thorough examination of the system configuration, automated and manual assessment of susceptibilities and vulnerabilities identified in previous IOVSA efforts, a reliability analysis of operating system and application software, and appropriate system/network exploits. Also, susceptibilities introduced by application programs are assessed and analyzed in the process.

The purpose of a laboratory or field IO experiment would be to:

- a. Identify potential IT-based system susceptibilities (operating system, system specific and mandated applications, network connectivity, etc).
- b. Evaluate the effectiveness of U.S. Army command and control Protect tools.
- c. Determine survivability of a weapons systems' platform under specific IO attacks.
- d. Provide protection assessment with recommendations on those IO threats that impact survivability.

Typically, during a laboratory or field IO experiment, in terms of the SoS network structure of a single vehicle and the larger SoS for networked battlefield architectures, the following functions are addressed:

- a. Users, operators, and administrators
- b. Application software
- c. Middleware
- d. Data base management systems (DBMS)
- e. Data communication equipment (DCE)
- f. Networking
- g. Operating systems
- h. Hardware
- i. Defense Information Infrastructure Common Operating Environment (DIICOE)
- j. Army Battle Command System (ABCS) foundation products

2.4.2 Rationale

The susceptibility assessment is required to determine the set of susceptibilities that are present in the system/SoS under evaluation. Whether each component of the susceptibility phase is performed is determined typically during phase I of the IOVSA process. Thus, depending on the type of system(s) (complexity) under evaluation, it may be determined that an experimental assessment will suffice. For other systems, a complete information flow model may be required to properly assess the system's susceptibilities.

2.4.3 Objectives

The objective of this activity is to identify the susceptibilities of a system to validated and/or technologically feasible threats. The susceptibilities defined in this part of the analysis will be used to define the vulnerabilities of the system in the vulnerability risk assessment phase V of the IOVSA process.

2.4.4 Deliverables

Deliverables for this phase of the IOVSA process are dependent on which blocks of the phase are executed. Typically, for systems that require modeling and simulation, a report for each of the analytical assessments as well as the modeling and simulation process is to be provided. For most systems, experimentation reports typically include the results of the analysis of the system under laboratory conditions, or (may even include the results from) evaluations performed on as-

fielded configurations. In all cases, the reports typically list the susceptibilities of the system that form the basis for the vulnerability risk assessment.

2.5 Phase V: Vulnerability Risk Assessment

2.5.1 Introduction

Vulnerabilities are the intersection of the sets of susceptibilities and threats. For the vulnerability risk assessment, SLAD compares the list of system susceptibilities (generated in phase IV), to the threats (identified in phase III). Susceptibilities that can be exploited by the threat are identified as vulnerabilities. For these susceptibilities, the probability that the system will encounter the particular threat must be greater than zero. This process may reduce the size and, therefore, the cost of protecting the system, since the number of vulnerabilities is always smaller than or equal to the list of susceptibilities.

In the greatest simplification, a vulnerability risk assessment is (nothing more than) a susceptibility assessment in which the likelihood of encountering all relevant threats is an event with the probability of one. The challenge is to accurately determine the probability of encounter for each threat.

If threat intelligence data is unavailable, the SLAD analyst will determine a reasonable estimate for the probability of encounter for each threat defined in phase IV. In addition, the analyst must attribute a degree of confidence in the risk calculated for each susceptibility/threat combination.

Based upon the results of the vulnerability risk assessment, SLAD will make appropriate protection recommendations to enhance system survivability. SLAD maintains a laboratory to test the protection mechanisms available from commercial and research institutions. This laboratory also provides a test bed for performing research and development to extend and modify products to suit the customer's needs.

2.5.2 Rationale

The importance of this section is found in the allocation of resources by the customer to correct the deficiencies found during the IOVSA process. A vulnerability risk assessment provides the PM with a list of vulnerabilities of the system, along with a likelihood of threat exploitation and a confidence level for the findings. Additionally, the report includes TTPs that address the IA criteria of concern.

2.5.3 Objectives

The objective of this phase is to identify susceptibilities that may become vulnerabilities based upon the likelihood of encounter. The likelihood of encounter encompasses factors such as the operational environment, method of deployment, and TTPs. The resulting measure will be an estimation calculated by the analyst when no such factor is available from the intelligence community.

2.5.4 Deliverables

The vulnerability risk assessment will be documented in a report. The recommendations to mitigate the threats will fall into three categories: (1) elimination of a susceptibility or vulnerability, (2) mitigation of a vulnerability without elimination of the susceptibility, and (3) reduction of a susceptibility or vulnerability with a risk management evaluation of any residual risk.

3. DITSCAP

The DITSCAP establishes a standard process, set of activities, general task descriptions, and management structure to certify and accredit systems that will maintain the security posture of the Defense Information Infrastructure (DII). The DITSCAP focuses on protecting the DII by presenting an infrastructure-centric approach for certification and accreditation (C&A). The DITSCAP is designed to be adaptable to any type of IT and any computing environment and mission. The process should be adapted to include existing system certifications and evaluated products. The IOVSA process fulfills the DITSCAP methodology for phases I, II, and III. Table 2 maps the steps of the IOVSA to particular DITSCAP process activities.

The DITSCAP is designed to certify that the system meets accreditation requirements and that the system will continue to maintain the accredited security posture throughout the system's life cycle. The users of the system will align the process with the program strategy and integrate process activities into the system life cycle. While DITSCAP maps to any system life cycle process, its four phases are independent of the life cycle strategy.

The key to the DITSCAP is the agreement between the system PM, the Designated Approval Authority (DAA), the Certification Agent (CA), and the user representative. These managers (or "players" per the DITSCAP CD-ROM) resolve critical schedule, budget, security, functionality, and performance issues. This agreement is documented in the system security authorization agreement (SSAA) that is used to guide and document the results of the C&A. The objective is to use the SSAA to establish a binding agreement on the level of security required before the system development begins, or changes to a system are made (4).

Although SLAD's IOVSA methodology can satisfy many of the DITSCAP requirements, it should be pointed out that the focus of DITSCAP is on security policy, whereas the focus of SLAD's IOVSA is on susceptibility/vulnerability and hence the overall survivability of a system/SoS.

Table 2. Relationship of the IOVSA methodology process to DITSCAP phases, activities and tasks.

| DITSCAP | | | ARL/SLAD |
|------------------|---------------------------------------|---|----------------|
| Phase | Activities | Task | IOVSA Phase |
| I. Definition | Document mission need | Determine and document mission functions | I |
| | Conduct registration | Register the system - inform the DAA and the user representative that a system will require C&A support | |
| | | Prepare mission description and system identification | I |
| | | Prepare environment and threat description | III |
| | | Prepare system architecture description | I |
| | | Determine the Information Technology Security (ITSEC) class | |
| | | Determine the system security requirements | I |
| | | Identify organizations that will support the C&A | |
| | | Tailor the DITSCAP tasks, determine the C&A scope, level-of-effort, and prepare the DITSCAP plan | |
| | | Develop the draft SSAA | |
| | Perform negotiation | Review the draft SSAA | |
| | | Conduct the Certifications Requirements Review (CRR) | |
| | | Approve the SSAA | |
| | Prepare the SSAA | | |
| II. Verification | Refine the SSAA | | |
| | Support system development activities | | |
| | Perform certification analysis | System architecture analysis | II |
| | | Software design analysis | II |
| | | Network connection rule compliance analysis | IV |
| | | Integrity of integrated products analysis | I, II, III, IV |
| | | Life cycle management analysis | I,II |
| | | Vulnerability assessment analysis | V |

Table 2. Relationship of the IOVSA methodology process to DITSCAP phases, activities and tasks (continued).

| DITSCAP | | | ARL/SLAD |
|------------------------|---|--|-------------|
| Phase | Activities | Task | IOVSA Phase |
| | Assess analysis results against SSAA requirements | | |
| III. Validation | Refine the SSAA | | |
| | Certification evaluation of the integrated system | Security Testing and Evaluation (ST&E) | IV |
| | | Penetration testing | IV |
| | | TEMPEST and red-black verification | |
| | | Validation of Communication Security (COMSEC) compliance | |
| | | System management analysis | |
| | | Contingency plan evaluation | IV |
| | | Risk-based management review | V |
| | Develop recommendation to the DAA | CA's recommendation | IV, V |
| | DAA accreditation | | |
| IV. Post accreditation | Maintenance of the SSAA | Review the SSAA | |
| | | Obtain approval of changes | |
| | | Document changes | |
| | System operation | System maintenance | |
| | | System security management | |
| | | Contingency planning | |
| | | | |
| | Change management | Support system configuration management | |
| | | Risk-based management review | |
| | Compliance validation | Review the SSAA | |
| | | Physical security analysis | |
| | | Procedural analysis | |
| | | Risk-based management review | |

Thus, as can be seen, the IOVSA methodology process can be used to prepare the system for the DITSCAP accreditation process.

4. Conclusion

This document is a revision of the IOVSA methodology formalized in June 2000. The goal of this revised document has been the clarification of the intended work to be performed for each phase, the requirements, and the expected deliverables. Since this revision is considered a living document, it will be updated as appropriate to include lessons learned. The intent of this revision is to facilitate the dialog between ARL/SLAD and the decision-makers (PEOs, PMs, evaluators, contractors, etc.) for U.S. Army IT-based systems.

As before, the IOVSA process provides a structured methodology for assessing IT system/SoS IO susceptibilities and vulnerabilities. The process provides flexibility that enables the analyst to customize it for the system/SoS under assessment. Additionally, the IOVSA results provide critical information to system developers and decision-makers regarding the system's/SoS' IO susceptibilities and vulnerabilities. Furthermore, enough information can be extracted from the process to evaluate different countermeasure techniques and protection recommendations to determine their feasibility and cost/reward ratio.

In summary, the IOVSA process provides the framework for a consistent and rigorous vulnerability assessment of a system/SoS in order to determine its IO areas of concern, and to discern the appropriate actions to protect and enhance soldier and system survivability.

References

1. *DoD Information Technology Security Certification and Accreditation Process (DITSCAP)*; 5200.40, 30; U.S. Department of Defense: Fort Monmouth, NJ, 1997.
2. Rick zum Brunnen, et al; *Information Operations Vulnerability/Survivability Assessment (IOVSA): Process Structure*; ARL-TR-2250, U.S. Army Research Laboratory: Aberdeen Proving Ground, MD, 2000.
3. *Information Operations*; FM 100-6; U.S. Department of Army: Washington, D.C., 1996.
4. *Defense Information Technology Security Certification and Accreditation Process (DITSCAP) Application Document (Draft)*, CORBETT Technologies, Inc, to be published.

Acronyms

| | |
|---------|---|
| ABCS | Army Battle Command System |
| ARL | Army Research Laboratory |
| ASAS | All Source Analysis System |
| C&A | Certification and Accreditation |
| CA | Certification Agent |
| CERT | Computer Emergency Response Teams |
| COMSEC | Communication Security |
| CRR | Certification Requirements Review |
| CSSCS | Combat Service Support Control System |
| DA | Department of the Army |
| DAA | Designated Approval Authority |
| DARPA | Defense Advanced Research Projects Agency |
| DBMS | Data Base Management Systems |
| DCE | Data Communication Equipment |
| DEW | Directed Energy Weapons |
| DII | Defense Information Infrastructure |
| DIICOE | Defense Information Infrastructure Common Operating Environment |
| DITSCAP | DoD Information Technology Security Certification and Accreditation Process |
| DoD | Department of Defense |
| EMP | Nuclear Electromagnetic Pulse |
| FBCB2 | Force XXI Battle Command Battalion/Brigade and Below |
| HQDA | Headquarters Department of the Army |
| IA | Information Assurance |
| IO | Information Operations |

| | |
|--------|---|
| IOVSA | Information Operations Vulnerability/Survivability Assessment |
| IT | Information Technology |
| ITSEC | Information Technology Security |
| LSI | Lead System Integrator |
| M&S | Modeling and Simulation |
| PEO | Program Executive Office |
| PM | Project Manager |
| RINT | Radiation Intelligence |
| SIGINT | Signal Intelligence |
| SIL | System integration Laboratory |
| SLAD | Survivability/Lethality Analysis Directorate |
| SLV | Survivability, Lethality, and Vulnerability |
| SoS | System of Systems |
| SSAA | System Security Authorization Agreement |
| ST&E | Security Testing & Evaluation |
| TMM | Tools, Models, and Methodologies |
| TTP | Training, Tactics, and Procedures |

